

IDNewswire

Trends in Personal Identification and Biometrics

www.cardtechnology.com

Vol. 2 No. 11 May 28, 2003

Workers Give Out Passwords Pg. 3

Office workers were persuaded to divulge their corporate passwords in return for no more than a free pen, a recent study shows.

Consumers Warm To Biometrics Pg. 4

A recent consumer survey shows ATM users find biometrics more attractive than PINs.

UAE Tests Facial Biometrics Pg. 4

Biometric Experts Skeptical Of Two Prints For Border Security

The U.S. Department of Homeland Security's decision to capture two fingerprint images from foreign travelers for the US VISIT program is raising some eyebrows in the biometric community.

Asa Hutchinson, Undersecretary for Homeland Security, says that visitors from non-Visa Waiver countries entering the country by January 1, 2004, will have their photos and fingerprints taken and then checked against a watch list of individuals not welcome in the United States. The biometric information will be checked again

when the visitor leaves the country to verify departure. Between 5 million and 6 million travelers a year enter the United States from countries other than the 27 nations whose citizens can come to the United States without a visa.

Using only two fingerprints could be time-consuming, depending on the size of the watch list checked, according to industry experts. Also, two fingerprints might not provide enough information to correctly identify someone on a watch list. "There are schools of thought that say

two fingerprints are not enough," says Joseph Atick, president and CEO of Minnetonka, Minn.-based Identix Inc, a biometric vendor.

The former Immigration and Naturalization Service captured two fingerprints from individuals caught entering the country illegally from Mexico, allowing INS to later identify an expellee trying to return. This was one of many uses for the INS' fingerprint system. However, a National Institute of Standards and Technology report issued in January recommended using all 10 fingerprints.

Most in the biometric industry

also say using 10 prints would be a better solution, allowing officials to have more information to run through a database to perform a background check. Another strategy would be to capture an applicant's biometric information and run a background check prior to visa issuance.

The government most likely will use technology known as Automated Fingerprint Identification System (AFIS) that is widely used by law enforcement officials to identify criminals. The FBI's "integrated" AFIS, > **US VISIT**, Page 2

ICAO Says PKI Will Protect Visas And Passports



The nations of the world are a step closer to knowing what standards they will need to meet for the next generation of passports and visas.

The International Civil Aviation Organization, a Montreal-based organization of 188 countries that sets standards for travel documents, is preparing to release a full report of its technical advisory group on machine-readable documents. Last week, ICAO's Air Transport Committee approved the advisory group's report on using facial biometrics and contactless chips. The organization is now working on finalizing the reports for publication.

The heart of the recommendation is that a 32-kilobyte contactless smart card chip should be embedded into passports and visas, and a digital photo of the document holder should be stored on the chip. The reports also states that facial recognition software will be used to match the document holder with the image on the chip.

While face will be the primary biometric, the ICAO

> **ICAO**, Page 3

Financial Services Hear Call Of Voice Biometrics

The financial services industry normally trails the government and health care industries when it comes to interest in biometric technology. But there are some examples of major financial service players testing biometrics, with an eye to using the technology as a way to offer innovative products in the future.

San Francisco-based Visa International is trying out biometrics on its employees. And, Boston-based Fidelity Investments has been testing different biometrics to secure a customer's transaction for three years.

Visa is rolling out a system that would allow Visa employees to reset their computer passwords by calling into a phone number and being authenticated by their voice, says Georgann Scally, vice president of strategic alliances at Visa International.

If an employee forgets a computer password, instead of calling a help desk, he or she calls into an automated phone system. The employee enters their employee ID number, and then they are authenticated by speaking a password or pass phrase. The voiceprint is matched against one previously stored upon enrollment. If the print is accepted, the employee is asked what they would like to change

> **Financial Services**, Page 4



IBG Analyzes Recent Biometric Tests

The International Biometric Group looks at two recent testing initiatives from iris recognition vendor Iridian Technologies regarding false matching and system response time.

> **IBG**, Page 5

Johnson Out At Datacard Group

Datacard, a provider of card-printing and issuance systems, fired its president and CEO, Jerry Johnson. Johnson had lead Datacard since June 1999.

> **Datacard**, Page 4

> US VISIT, Page 1

or IAFIS, is the largest such system in the world and holds roughly 50 million sets of fingerprints.

AFIS uses algorithms to calculate points on the fingerprint image and then compares those points against others for identification purposes. This differs from other fingerprint biometric systems that use algorithms to translate points on the fingerprint, or the entire fingerprint image, into a template, or a string of numbers.

While AFIS is considered more reliable and tested than other biometrics, its reliability running a check of two fingerprints against a watch list database of more than 10 million sets of prints is unknown, says Charlie Wilson, manager of the imaging group in the information access division at NIST. "I've been working in fingerprints for 12 years and this is as complicated a system as I've ever seen," he says.

Some of the complications include the wide variation in the quality, type, and number of the fingerprint images stored in the different government databases, Wilson says. "The image quality goes from pretty good to pretty awful," Wilson says. "Truth is the U.S. government has more flavors of fingerprints than Baskin-Robbins."

The FBI's IAFIS stores "rolled 10-prints," all of an individual's fingerprints that are rolled on a sensor to provide a greater surface area and more information for a potential match. A rolled print will have 70 to 170 minutia points for identification, according to Robert Christensen, senior vice president at Cross Match Technologies Inc, a Palm Beach Gardens, Fla.-based fingerprint vendor.

Flat prints are the other option. This is what the INS used, and what is being proposed for US VISIT. Flat prints capture 34 to 100 minutia points, Christensen says. Rolled 10-prints basically offer ten times the information to search with and thus greater accuracy.

"When you have flat fingerprints and it's only two it offers limited minutia data and it lengthens the search time," he says.

Exactly what kind of a background check will be done at the border is not yet known. But if the database of fingerprints is of considerable size, wait times could be significant. "Two fingerprints would work if the size of the lookout database was kept reasonably controlled," says Denny Carlton, director of Washington operations for the International Biometric Group. "You can't have tens of hundreds of millions of records."

A database of 3 million fingerprint records would require human operators to resolve matches using two fingerprints because of the amount of information present, says Identix's Atick. Searches of IAFIS' 50 million records take a couple of hours to complete, Wilson says. There are about 90,000 searches per day, he says.

With immigration agents capturing fingerprints via scanners at all 395 ports of entry into the country it is likely that US VISIT will quickly become the largest two-print biometric database in existence, says Tom Larson, vice president of strategic development at France-based Sagem Morpho, an AFIS provider.

This means watch-list checks at border crossings may become more time-consuming. Visitors to the U.S. will submit their fingerprints, which will then be run through AFIS for a background check. Depending on the size of the database checked, this process could take a couple of minutes or a couple of hours. Larson suggests performing background checks when the traveler applies for a visa, instead of at the border.

As the U.S. State Department gears up to begin issuing machine-readable biometrics on all visas, what's most likely to happen is the background check will be done during the visa interview process. Individual applying for

a visa at one of the 210 embassies or consulates around the world will have their biometric information taken and run against a watch list prior to visa issuance, Larson says.

If the traveler clears the system they will then be issued a visa with their biometric information stored in it. When the individual arrives in the United States the information contained in the visa will then be checked against the individual presenting the document. This would require the border officials to do a one-to-one match, which takes seconds, versus a one-to-many match, which can take hours.

Stuart Patt, spokesperson for the Bureau of Consular Affairs at the State Department, says details of the new visa-issuance process are still being

worked out. However, facial recognition will be a part of the new visa issuance process because of the recommendations from the International Civil Aviation Organization. Montreal-based ICAO recommended that facial recognition biometrics be used in travel documents, while also offering guidelines for fingerprints and iris biometrics. (*See Travel Documents, Page 1.*) It is likely the State Department will use another biometric as well, most likely fingerprints, according to a State Department official.

The State Department is already increasing the number of face-to-face interviews that take place during the visa-application process, Patt says. As many as 90% of visa applicants will be interviewed by consular officers before a visa is granted to help improve the security of the visa-issuance process, he says.

Another possible scenario would be for travelers to submit biometric information before boarding the plane at their departure airport, says IBG's Carlton. "If you capture the prints when they get on the plane you could do the check while they are traveling," Carlton says.

Homeland Security is expected to issue a proposal for US VISIT to vendors and systems integrators in September. Hutchinson says the system will be in place at some ports of entry late this year and early 2004. "It's an aggressive schedule because the procurement process is likely to take a long time," says Carlton. Large pilot programs are likely at first, rather than a full-scale rollout, Carlton says. "Nobody has tried something like this with these combinations of factors before," he says. <

'There are schools of thought that say two fingerprints are not enough.'

— Joseph Atick, Identix Inc.

US VISIT Facts

- **\$380 million appropriated for Fiscal Year 2003.**
- **Biometric identifiers must be consistent with ICAO standards.**
- **System will be capable of capturing biometrics at airports and seaports before the end of 2003.**
- **Proposal for system due to vendors and systems integrators some time in September.**

Office Workers Fall For Social Engineering

Office workers passing through London's Waterloo Station in April were persuaded to divulge their corporate passwords in return for no more than a free pen.

Using social engineering techniques, researchers from the Infosecurity IT security exhibition were able to extract confidential and sensitive information from more than 90% of the workers they interviewed. That number was up from 65% a year ago, when a similar study was carried out.

Of the 152 office workers surveyed, many offered additional personal information and explained the origin of their password. For example, "my car – Celica," "my football team – Arsenal," "my name – Cynthia," "my pet's name – Dribbles." The most common password was "password," 12%, and most popular category was their own name, 16%, followed by their football team, 11%, and date of birth, 8%.

"I am the CEO, I will not give you my password, it could compromise my company's information," one man told a researcher. However, later in the conversation, he revealed that his password was his daughter's name. "And what is your daughter's name?" the interviewer asked, to which he replied "Tasmin."

Given their willingness to divulge their "secret" passwords to strangers, it's hardly surprising that colleagues tend to share passwords with each other. Two-thirds of the workers say that they have given their passwords to a colleague, and three-quarters knew their co-workers' passwords.

"We all use the same password so we can remind each other if we forget, or we need to get into someone's computer when they are on holiday," said one woman.

A man who said he works in the IT department of a travel agency said, "We keep as many passwords as possible at the default that comes with the software, such as 'admin' or 'password', so that we do not need to keep remembering them. I log onto different applications and networks around a hundred times a day; it is a nightmare to remember all the passwords."

And it isn't just corporate security that is at risk. In addition to using their password to gain access to company information, two-thirds of workers say they use the same passwords for everything, including personal banking and Web access. <

> ICAO, Page 1

document leaves open the possibility for countries to use fingerprint and iris recognition with travel documents, as well. ICAO chose facial recognition as the primary biometric largely because border control authorities and airline staffs already use photographs to confirm identity. The ICAO documents says a 32K chip should be used, but there is discussion that U.S. officials might want to use a much larger chip.

One of the more challenging tasks associated with adding contactless computer chips to travel documents will be protecting the data stored on the chip. Safeguards must be put into place so that only authorized individuals can read that information.

The ICAO documents refer to a "modified public key infrastructure" that will provide security against unauthorized alteration or access. There is also a call for a standard data structure so information stored by one country can be read by another.

The PKI used for travel documents, like standard PKI systems, would use a pair of keys, a public one and a private one, according to Mary McMunn, chief of ICAO's facilitation section. Each key is a string of random characters that is combined with an algorithm to encrypt and decrypt data. "The key encrypts the data and provides a digital signature which would be a way of validating the data," she says.

For example, a country issuing a document would encrypt data it stores on the chip with its private key. When the traveler arrives in another country, that country will look up the issuing authority's public key and use it to decrypt the data.

ICAO recommends countries change their key pairs periodically. Other countries will be able to find the corresponding key by when the document was issued, McMunn says. ICAO may act as a repository for all participating countries keys, McMunn says.

What makes this "modified PKI" is that there might not be one central key-issuing authority, according to Chuck Baggeroer, director of security, technology and industry liaison at the Datacard Group, and an observer to the

ICAO committee. ICAO may act as the central repository for all public keys. Otherwise, countries would have to find another system to share them with one another.

One caveat with PKI is the risk of a country's private key being hacked or made publicly available. If this happens, all documents using that key would have to be reissued.

Neville Pattinson, director of business development and technology at SchlumbergerSema, says the private key used would have to be kept secure. "The private key would be heavily protected with no mechanism to extract it," he says. Countries would have to use long key lengths in order to prevent hacking.

How much a PKI system like this would cost is unknown. One clue comes from the U.S. Department of Defense, which uses PKI with its Common Access Card, a smart card ID being issued to 4 million defense and civilian personnel. The management and issuing of digital certificates in that case is expected to cost \$712 million through 2005.

However, costs of integrating PKI into many systems may have contributed to the high cost for the Pentagon.

Security of the information on the chip is a primary concern, but the size of the chip countries use may also be an issue. ICAO recommends 32K chips as a memory size.

However, government and industry officials are now saying the United States may want passports to contain a 512-kilobyte chip. A U.S. government official says the U.S. could possibly want passports to store raw images of 10 fingers, two irises, and a facial image.

Raw images would need to be stored, instead of templates, because of the lack of standards for biometric templates between vendors.

A possible issue with using a 512K chip is there is only one manufacturer, Japan-based Sharp Electronics Corp., which is known to have a contactless chip that large.

Sharp has been testing a one-megabyte chip in a government identification program in Japan. Robert Stuart, product manager for Sharp Microelectronics of the Americas, says the 512K chip would cost around \$6 or \$7. <

One caveat with PKI is the risk of a country's private key being hacked or made publicly available.

> Financial Services, Page 1
their password to.

Visa is using voice biometric technology from Mountain View, Calif.-based Vocent Solutions Inc. Visa and Vocent also have a partnership to look at using voice authentication in consumer settings as well. "If we can authenticate ourselves on a mobile phone as we are performing commerce, rather than keying things in, it would be easier," Scally says.

Vocent has seen interest in voice biometrics from others in the financial services industry, says Chuck Buffum, CEO of Vocent. "Password reset is the easiest entry point and is the safest way to start using the technology," he says. A recent report from San Francisco-based Glenbrook Partners report calls voice recognition for changing passwords a "no-brainer application" and a good way for financial services companies to get started with biometrics.

Voice biometrics could be a key technology for the financial services industry, as consumers are already accustomed to calling

their banks to check balance and other account information. Buffum says voice recognition could make those transactions more secure, or at least speed up interactions with customer service representatives.

Currently, when consumers call into a customer service center they sometimes must run through name, address, Social Security number, and other information before the representative proceeds with the request. Buffum says voice recognition can allow a consumer to be authenticated before talking to the rep, saving both parties time.

Vocent is in the process of rolling out a pilot using this type of a system for a large financial services provider, though Buffum could not release the client's name.

While biometrics may be new for some in the financial services industry, Fidelity Investments has been looking at biometrics for the past three years, says Charlie Brenner, senior vice president at Fidelity. "People want convenient access on the one hand, but highly secure access on the other, and those two things are fundamentally at odds with one

another," he says. "Our customers are worried about security and identity theft, and the anxiety around these are growing."

While customers are not specifically asking for biometrics, they want another layer of strong security that is easy to use, Brenner says. "Biometrics is one way to break that log-jam and create a system that is easy and secure," he says.

But Brenner says he is still looking for the right technology. "What we are always in search for is a biometric that is universally available and inexpensive and convenient enough for all our members," Brenner says. "For years we have believed that something will arise in the biometric hardware industry that would become a standard. It's obvious that hasn't come to pass and may never."

As of late, Fidelity has noticed the availability of cheap cameras and is looking at using facial recognition for customer authentication. The company also runs a lab where consumers test different security products, including biometrics, while viewing Web sites, Brenner says. <

Consumers Warming To Biometrics

A recent consumer survey shows ATM users find biometrics more attractive than personal identification numbers, according to the study by Synergistics Research Corp. Fingerprint or handprint scanning is the preference of more than four in ten ATM users. Some 25% say iris recognition would be preferable, while 10% liked voice recognition. When asked which types of security measures would be an improvement over using their ATM card and PIN, 77% of users indicated they find biometrics to be an improvement. <

UAE Airport Tests Facial Biometrics

Littleton, Mass.-based Viisage Technology Inc. announced that the company will partic-

ipate in a security project with the United Arab Emirates Ministry of Interior that uses Viisage facial recognition technology at Dubai International Airport. The technology will be used to spot identity fraud by visa applicants, as well as checking individuals against a watch list of known terrorists or wanted felons. <

Datacard Fires CEO Jerry Johnson

Datacard Group, a major provider of card-printing and issuance systems, has fired its president and CEO, Jerry Johnson. "The board of directors has determined that in order to move more quickly on driving performance and growth, a CEO change was indicated," says Kevin Gillick, head of corporate marketing at privately held Datacard. He

says the chairman of the board, Hatim Tyabji, would serve as interim CEO while the company searches for a successor. That search is expected to take four to six months, he says. Gillick says the company recorded growth in all its business segments in its fiscal year that ended March 31, but did not provide details. However, an industry source says Johnson's departure was not unexpected as the company's financial results were not meeting the board's expectations and the company was cutting staff and closing offices to cut costs. Gillick confirms Datacard laid off just over 10% of its work force in April, reducing head count to 1,200 worldwide, and consolidated operations in Canada, France and Germany. Johnson had led Datacard since June 1999. <

Editor**Zack Martin**zachary.martin@thomsonmedia.com**Group Editor****Donald Davis**don.davis@thomsonmedia.com**Contributing Editor****Michael Fenner**michael.fenner@thomsonmedia.com**Advertising Sales****Jim Baker**james.baker@thomsonmedia.com**Publisher****Robert Jenisch**robert.jenisch@thomsonmedia.com**Group Publisher****Timothy Murphy**timothy.murphy@thomsonmedia.com

Thomson Media: CEO: Robert Cullen; President/CEO Publishing & Conference Group: Bruce Morris; CFO: William Johnston; SVP, Operations: Celie Baussan; CTO: Raymond Ouellette; VP, Business Development and Strategy: Greg Mazzanobile; VP, Human Resources: Robert DeNoia.

IDNewswire is published biweekly by Thomson Media. Visit our Web site at <http://www.cardtechnology.com>. The contents of IDNewswire are, and remain, the property of Thomson Media. Reproduction or forwarding of this publication is strictly prohibited. Individuals who infringe on these rights will be prosecuted to the full extent of the law.

Subscribers who want multiple copies of IDNewswire should contact Barbara Mahin at 212-803-8768 or barbara.mahin@thomsonmedia.com for information. The annual subscription rate is \$695. For subscription, renewal or licensing information, please contact Barbara Mahin at 212-803-8768 or barbara.mahin@thomsonmedia.com.

For advertising information, contact Jim Baker at 312-983-6179 or james.baker@thomsonmedia.com. Editorial offices are located at 300 S. Wacker Drive, 18th Floor, Chicago, IL 60606. Telephone: 312-983-6168. FAX: 312-913-1365.

© 2003 The Thomson Corporation and IDNewswire. All rights reserved.

IBG Reviews Iridian's Recent Testing Initiatives

The following is the second half of an edited transcript from the May 8 International Biometric Group's teleconference by Michael Theime. In the May 14 IDNewswire Theime discussed the results of recent government biometric tests.

The third test that we want to talk about is from Iridian. It is a test of iris recognition technology entitled the Iridian Cross Comparison Test, published in December 2002. This testing was designed to determine how resistant iris recognition technology is to false matching.

A very notable aspect of this testing is that a much larger database was used than had ever been used prior. Approximately 120,000 templates were used, whereas previously the largest tests ran from a few hundred up to perhaps a few thousand individuals. The new testing is orders of magnitude larger than that which occurred before.

In terms of the methodology utilized in Iridian's testing, 120,000 iris templates, or iris codes, were collected from around the world from different implementations. This is real-world data, not collected in a test lab.

Iridian created nine target databases of between approximately 7,000 and 17,000 users. Against these target databases was tested a 9,000-person probe database. It happens that the 9,000-person probe database was collected from an implementation in Iceland. With a 9,000-person database searching against these various other databases, what results is approximately 983,000,000 cross comparisons. This provides a very large number from which to base false match data.

What Iridian found and published pertaining to false matches at different thresholds was interesting. Testing indicates that there are certain thresholds at which false matches will occur with iris recognition technology. Reducing the threshold as databases get larger offsets the false-match.

Specifically what was reported was that at the 0.31 threshold, or the 0.31 hamming distance, there were 157 cases in which two different templates matched. That dropped to 32 when you moved to one threshold of higher security down to only one error at what was called the 0.27 threshold. What this tells us is that there is a band or a point at which the threshold needs to be set in order to eliminate or reduce the possibility of a false match in iris recognition technology.

These results – which certainly bode well for the accuracy level of the technology – come with a condition: there was no corresponding false non-match rate testing. So what we have, essentially, is half the equation. It is an important half, and it is great data to have. But in order to really understand, for example, whether a 0.29 threshold will do the job in the real world, we need to understand whether or not you are going to get a lot of false non-matches at the 0.29 thresholds. And certainly we eagerly

International Biometric Group

anticipate that there would be that additional data, so that we understand that these thresholds are what can be used in the real world.

In terms of additional testing areas relating to iris recognition technology, I think an important measurement will be the false non-

match rate over time.

A day-one false non-match rate may differ substantially from a day-180 or a day-360-plus false non-match rate. That is a particularly important piece of data. The second piece not included in this testing, and which I think is an important measure for this technology specifically, is the failure-to-enroll rate.

By definition, any-

body who was included in this particular cross comparison test would enroll, as testing was based on an operational database. However, there are individuals who have difficulty interacting with this system and positioning themselves correctly. So an important metric to be generated here in some sort of real world environment will be the FTE rate.

Another area that will provide a basis for further Iridian and iris recognition testing is the error rate for different input technologies. An important trend that has emerged in this field over the last 18 months is the fact that we have a number of technology suppliers who will provide different types of iris devices – all based on the same core Iridian technology, using different imaging methods. We are referring to companies such as Panasonic, LG, and OKI. I think it will be very important to understand whether enrollment and identification in different devices will produce different results.

And one last point may be interesting to study. The data presented in the cross comparison test seems based on enrollment images. Normally, enrollment in Iridian's technology requires the acquisition of multiple

'It will be interesting to investigate error rates of a single image, the concept of operations of somebody who is just going up to a door or up to an access point looking to be identified. The question is, will the error rates be higher than with just the single image identification?'

Iridian Cross Testing Comparison Information

- **Nine target databases, between 7,000 and 17,000 users.**
- **Target databases were tested against a 9,000-person database.**
- **Resulted in approximately 983,000,000 cross comparisons, providing a large number from which to base false match data.**
- **Testing indicates that there are certain thresholds where false matches will occur. Reducing the threshold as databases get larger offsets the false-match.**

> **IBG, Page 5**

images so that you build or develop a high-quality code. It will be interesting to investigate error rates of a single image, the concept of operations of somebody who is just going up to a door or up to an access point looking to be identified. The question is, will the error rates be higher than with just the single image identification?

And the last test we will talk about today is another Iridian test: the Iridian Scalability Test. This test is different than what we talked about before inasmuch as it measures performance in terms of speed and in terms of response time as opposed to accuracy. We should note that response time and speed is an area of biometric testing that has

been largely overlooked. The publication of these results is most welcome, and we hope to see similar studies with similar documentation from other technology providers.

The objective of Iridian's scalability test was to assess the response time for both identification and enrollment. Testing also addressed increased transaction loads and different hardware configurations. What we found is the results strongly suggest that match speed may be an even bigger differentiator for iris recognition technology compared to fingerprint technology.

That is, iris recognition technology is known to be accurate – and certainly we are still establishing the degree to which it is accurate – but it also seems to have the advantage of working fairly quickly for a large-scale database with a relatively small amount of processing power.

We will talk briefly about the methodology and skip to the results. Iridian duplicated 450 templates multiple times to create large databases of one million people. Then, target templates were inserted at various points in the database – such that the system would need to search 100,000, 500,000 or 1,000,000

records. Once the target record is located one knows the transaction time, as you know how many records were searched.

Iridian measured transaction time for identification and enrollment, and they also measured in terms of the times it took to perform different functions. The functions identified were network transmission time, API time, and manager time. The manager time is the actual algorithm processing, which is proba-

bly of the greatest interest to most people.

In terms of the results presented, what we will discuss are worst-case scenario results, when the last person in the database (e.g. the one-millionth enrollees) is located. A single identification request against a one million-person

database was returned in 3.5 seconds on a faster platform and was returned in 5.8 seconds on a slower platform. So we are talking about a one to one million search conducted and executed in 3.5 seconds. This is somewhat faster than what we have come to anticipate in the biometric industry. This is notable when one considers the corresponding accuracy.

When a system is loaded with ten simultaneous transactions, meaning that when ten different people are being identified from ten separate clients backed up to the same server: the recognition time approximately triples.

What that means is that you are looking at approximately a 10-to-20-second response time for one million enrollees. This transaction time increased directly as a function of database size. In terms of enrollment time, enrollment was slightly more time-consuming. Enrollment in a one million-person database required approximately six seconds.

Now keep in mind that this is not measuring time to actually provide the data on the part of the end-user, we are talking about the time to take adequate iris code into the data base beginning to end. Now in this particular test, the results were only provided for the slower

processor. They did a test of these systems on a 933 and also on a 2.2 gigahertz system. So we are not sure how much faster the enrollment would have been on a faster platform.

One thing to know in terms of mapping these results in real world application, in almost every environment you are going to conduct first a one-to-many identification prior to enrollment. In most cases, one searches the database before inserting the person in your database in those environments. In this situation, one is looking at the whole process requiring less than twelve seconds – again a pretty impressive figure.

One issue that was not addressed in the Iridian testing and which certainly warrants some consideration is: what happens when you are enrolling multiple people into the system at the same time? It will be beneficial to understand what happens when 10, 15, 20, or 30 people are attempting to enroll at the same time within the technology.

One reason why this is important is reflected in recent news stories about the potential use of iris recognition technology in passport applications, perhaps in the UK. If you take an application where you have to enroll 50 million people over a five-year period, that breaks down (assuming a relatively even distribution, which would never happen) to 83 people per minute. So the technology needs to be able to turn these enrollments around very quickly.

I think the question will be the degree to which the Iridian platform can be enhanced to the point where it can scale, perhaps using multiple servers or other types of methods where it can actually handle multiple enrollments per minute. Credit goes to Iridian for having provided this data to the industry and we certainly hope that more tests like this are forthcoming. <

For more information contact Michael Theime, at mtheime@biometricgroup.com or 212-809-9491.

International Biometric Group is hosting the BiometricsWorld Executive Conference on Biometric and Travel Documents: A Global Perspective on New Standards, Technologies and Applications, June 3-4 in Washington at the Renaissance Hotel. Speakers include Russ Neuman from the White House, Gary Strong from DHS, Rick Lazarick from TSA, and several others. Topics include the federal agenda for biometric research and privacy concerns with biometric and travel documents. For more information, go to www.biometricgroup.com.

One issue that was not addressed in the Iridian testing and which certainly warrants some consideration is: what happens when you are enrolling multiple people into the system at the same time? It will be beneficial to understand what happens when 10, 15, 20, or 30 people are attempting to enroll at the same time within the technology.